Testimony of

Timothy E. Roxey

Technical Assistant to President of Constellation Generation Group
Deputy to the Chair Nuclear Sector Coordinating Council
Deputy to the Chair Partnership for Critical Infrastructure Security

Before the Committee on Homeland Security
United States House of Representatives
Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology

The Cyber Threat to Control Systems: Stronger Regulations Are Necessary to Secure the Electric Grid.

October 17, 2007

Mr. Chairman and Members of the Subcommittee:

I am Tim Roxey, Technical Assistant to the President of Constellation Generation Group for security and Deputy to the Chairs for both the Nuclear Sector Coordinating Council (NSCC) and the Partnership for Critical Infrastructure Security (PCIS). I am also the team lead for the Aurora mitigation efforts for the Private Sector.

In this last role I collaborate with subject matter experts (SME) (Research Engineers from Idaho National Labs (INL) and their contractors…who discovered the present vulnerability, Industry SME from all of the impacted Critical Infrastructure Sectors, Department of Homeland Security (DHS) and Department of Energy (DOE) SME and officials) in order to develop mitigation strategies to thwart the exploitation of the cyber vulnerability which threatens our critical infrastructure. Before becoming a Technical Assistant and Deputy to the Chairs of NSCC and PCIS I was a director of IT at one of our Nation's Nuclear Power Plants. In this role I was responsible for all telecommunications, IT applications and Cyber Security for the entire nuclear fleet. In addition, I was the nuclear sector's Chairman of a standing committee dedicated to Cyber Security. I was a founding member of the Nuclear Energy Institute's (NEI) cyber security task force; formed shortly after 9/11, the task force's purpose was to write an assessment and mitigation guidance document for nuclear power plants. This document, NEI 04-04: Cyber Security Program for Power Reactors was endorsed by the NRC and found an acceptable method to address cyber security. Since the endorsement of NEI 04-04 the NRC has proposed regulations for cyber security that are consistent with NEI 04-04.

I have also had former senior level governmental interactions when I worked with Vice President Al Gores' National Performance Review as a private sector Industry Sector Liaison. In this capacity I was charged with bringing Industry's requirements for regulatory interactions into a discussion with various federal sector agencies.

I am here today however, to discuss the successful use of the Public-Private Partnership model discussed in the National Infrastructure Protection Plan (NIPP). This partnership brought about the mitigation of the recently identified control system vulnerability (CSV) without the need for significant regulatory action by any federal agency. My discussion will fall into two areas as they relate to the present vulnerability. These areas are:

1) Actions taken within the Public-Private partnership - structures and processes which reduce risk of vulnerability
2) Preliminary lessons learned – a look back on this effort to help improve the performance of the Public/Private Partnership model's performance.
3) Concluding Remarks

Actions Taken

The Nuclear Sector was approached by DHS about the Aurora vulnerability in February of 2007. At this initial briefing it was decided that a more through briefing would be given to a select sub-group of the NSCC. It was also stressed that this subject is very sensitive and hence needed to be protected from disclosure.

To this final point DHS worked very hard to make sure that the Aurora issue remained at a FOUO level rather than being classified at a higher level. This decision was based on the fact that it is the private sector that owns, operates, and secures roughly 85% of all of our nation's critical infrastructure and key resources. By having the knowledge of this vulnerability classified it would have been difficult if not impossible for the private sector to develop and implement mitigation strategies as rapidly as it has.

In late February DHS officials from Infrastructure Protection briefed the details of the Aurora vulnerability to the NSCC. At this meeting the nuclear sector decided to take aggressive action to develop and implement mitigations that would reduce the exposure of the nuclear power facilities to this vulnerability.

A multilevel structure was developed within the nuclear sector and individuals assigned. The structure consisted of an Executive Review Board that reported to the NSCC and a Technical Task Team that was charged with development of guidance document for industry to use to perform mitigation activities.

The nuclear sectors' Aurora Technical Team worked in close coordination with the Electric Sectors' technical team in the development of mitigation documents. The nuclear sectors Technical Team also worked in close coordination with its government partners including strong coordination with the NRC.

The various mitigation actions that were developed were divided into two areas. One area was short-term, mid-term, and long-term actions and the second area was a set of actions designed to be implemented immediately if the specific vulnerability was actually being exploited. It is gratifying to say that the immediate actions have not been needed. The shortest term actions were targeted at substantially reducing the exposure to the vulnerably and the longest term actions were designed to make improvements in the supply chain and stand up programmatic actions.

The support from DHS, DOE, and the national labs (such as Idaho National Labs) in the rapid development and implementation of these mitigation documents was essential. In addition DHS has maintained a strong presence with the nuclear sector throughout these mitigation efforts. This effort is an example of the very effective Public-Private partnership.

When the mitigation documents were completed they were routed through the NSCC and ESCC for approval and then scheduled for release to industry. The release of the Nuclear Sectors mitigation document was coordinated with the release of the Electric Sectors (ES) Information Sharing and Analysis Centers (ISAC) Advisory which was released one day after the Nuclear Sector mitigation document

Based on the endorsement of the NSCC, the Nuclear Sector Technical Task Team added additional resources such as a Project Manager to manage the actual implementation phase of the mitigation work. A kick off meeting was held in Washington DC on June 13 with a final release to the industry of mitigation documents made the following week.

Within the nuclear sector a series of weekly meetings between the nuclear sector Technical Team (comprised of representatives from INL, DHS, and Industry) and the

various points of contact for all of the nation's nuclear power plants was convened and mitigation efforts began. To monitor the sectors performance the Technical Task Teams' PM prepared status reports for the Executive Review Board and DHS. These reports were updated every week based on the weekly meeting report out by all of the nuclear utility participants.

Each of the sector mitigation documents urged that actions be taken within 60 days and then again different actions within 180 days. The NRC in a letter, coordinated for release along with the sectors' mitigation document, requested that the nuclear sector licensees provide an update to the NRC on progress made at the completion of the 60 days and 180 day efforts.

Why did Nuclear take this initiative on as a requirement? The nuclear power sector took this opportunity to demonstrate its commitment to security. The sector recognized the validity of the vulnerability, and because the sector is well structured to handle these types of emergent issues, with only 65 physical sites and 104 power plants and a well organized industry association (the Nuclear Energy Institute), it was feasible to develop a uniform mitigation plan that sector members could implement within the desired time frame.

Lessons Learned

1. **An effective, voluntary public-private partnership is the key to timely mitigation of security vulnerabilities.** Proactive industry actions, endorsed by a federal agency with oversight responsibilities, are effective in reducing the risk to our nation's nuclear infrastructure in a timely manner without the delays or exposure of sensitive information that the due process requirements of regulatory action could necessitate.
2. **Trust the technical experts and involve them in all communications.** Bring them along to meetings and briefings for support. Several times it seemed that the message changed as it moved from the technical experts to the policy experts. When non-technical people brief on technical aspects to technical people there is a high risk of losing credibility and it becomes difficult to recover.
3. **Bring in a vetted industry group ASAP to validate and partner with researchers**. This group will validate the conclusions of the researchers and facilitate expedient response by private sector owners and operators, because their involvement lends credibility to the message. Sector leads from PCIS may be an appropriate group, as long as they bring their technical experts to the table as well. In this regard, PCIS is an appropriate vehicle to ensure that there is a broad review across many sectors.
4. **A multi-sector implementation plan is needed to provide cross-sector coordination.** An implementation plan should be developed that addresses the sequence of sector engagement based upon a full discussion between the public sector and private sector. Although in the present effort this was performed successfully this step needs to be institutionalized so that future discoveries can benefit from this step. This plan should address the sector and assets to address first then second then third, etc.

5. **Consistent common messaging provides consistent common mitigation.** There should be a common message that all effected sectors receive. In this particular case there are mixed messages. After 16 months of research and 5 months of multi-sector mitigation strategy development there are still some messages saying this is not a significant issue because of the difficulty of exploiting it and others saying it is.
6. **Single point of contact facilitiates effective coordination.** The establishment of a single point of contact within DHS was of great utility to the Private Sector. This single point of DHS contact provide for consistent and sustained coordination with the subject matter experts of INL and the private sector team of subject matter experts and the Aurora Technical Team's lead. This support was instrumental in the achievement of nuclear sectors 60 day mitigation and the electric sectors mitigation of nearby electric sector assets.

Concluding Remarks

The course of action that is recommended for any future discovered vulnerability, in light of the success of the present mitigation efforts, leads to the conclusion that continued decisive and coordinated private sector partnerships leads to a better vetting of vulnerabilities and a faster response via mitigation. In addition, these actions can take place much faster than the regulatory rule making process. This was shown to be the case within the nuclear sector.

Additionally, the course of action that is recommended for any future discovered vulnerability, in light of the success of the present mitigation efforts, leads to the conclusion that continued decisive, coordinated, and committed effort by government, and private sector leadership within the framework of the Public Private Partnership model should be nurtured and continued. Early engagement of private sector leadership through interaction between DHS, PCIS and the vulnerability researchers is an excellent way to fully vet the emerging vulnerability with both DHS (and SME's from other federal agency's) and the private sector.

These efforts should start with effective awareness campaigns to educate all sectors about the risks that they currently face, followed with clear guidance on appropriate mitigation measures for the newly discovered risk. This guidance should contemplate all aspects of the technology lifecycle, including improved development standards, implementation guidelines, operations procedures, and incident response. Good progress has been made by progressive asset owners, industry-initiated infrastructure protection leadership and by vendors willing to anticipate larger market-driven requirements for more security. Security, including cyber security, is best enhanced by continuing to build trust relationships and voluntary coordination and cooperation using the sector partnership framework. The nimbleness that effective security requires in the modern world makes these trust relationships our best defense.